GIODO

Generalny Inspektor
Ochrony Danych Osobowych

Raport o ochronie danych osobowych

1. ŹRÓDŁA PRAWA W ZAKRESIE OCHRONY DANYCH OSOBOWYCH

Prawo międzynarodowe. Najstarszym aktem prawnym o zasięgu międzynarodowym, kompleksowo regulującym zagadnienia związane z ochroną danych osobowych jest Konwencja Rady Europy Nr 108 z dnia 28 stycznia 1981 r. o Ochronie Osób w Związku z Automatycznym Przetwarzaniem Danych Osobowych. Konwencja ta nałożyła na kraje członkowskie zobowiązanie stworzenia ustawodawstwa w zakresie ochrony danych osobowych, wskazując jednocześnie, w jakim kierunku ustawodawstwo to ma zmierzać. Celem Konwencji jest zapewnienie, na obszarze państw członkowskich, każdemu (niezależnie od obywatelstwa i miejsca zamieszkania) ochrony jego praw i wolności, a w szczególności prawa do poszanowania sfery osobistej, w związku z automatycznym przetwarzaniem danych osobowych. Konwencja Nr 108 została podpisana przez Polskę w kwietniu 1999 r. i ratyfikowana w maju 2002 r. (Dz. U. z 2003 r. Nr 3, poz. 25).

Prawo Unii Europejskiej. Początkowo Unia Europejska nie dostrzegała konieczności jednolitego uregulowania ochrony danych osobowych w aktach prawa krajowego. Komisja Europejska postulowała jedynie, aby państwa członkowskie ratyfikowały Konwencję Rady Europy Nr 108. Z czasem jednak rozbieżności w ustawodawstwach państw Unii spowodowały konieczność ich ujednolicenia. Zasadniczym zadaniem, jakie miała spełnić taka regulacja, było zapewnienie minimalnego, a zarazem wspólnego dla państw członkowskich poziomu ochrony danych osobowych gromadzonych w zbiorach oraz zapewnienie swobodnego przepływu danych osobowych pomiędzy krajami członkowskimi. W 1990 r. rozpoczęto prace nad stosowną dyrektywą. Efektem tych prac było wydanie dyrektywy Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. (95/46/WE) w sprawie ochrony osób w związku z przetwarzaniem danych osobowych oraz swobodnego przepływu tych danych. Termin na jej implementację do porządków prawnych państw członkowskich wyznaczono na 23 października 1998 r. Do dziś wyznacza ona ramy prawne ochrony danych osobowych w Unii Europejskiej (Dz. Urz. WE L 281 z 23.11.1995). Należy również wspomnieć o decyzji ramowej Rady 2008/977/WSiSW z dnia 27 listopada 2008 r. w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych (Dz. Urz. UE L 350/60 z 30.12.2008), która reguluje kwestie ochrony danych osobowych w dawnym III filarze UE. Po wejściu w życie Traktatu z Lizbony, w 2009 r., prawo do ochrony danych osobowych zostało wprost zagwarantowane w prawie pierwotnym tj. w art. 16 Traktatu o Funkcjonowaniu UE oraz w art. 8 Karty Praw Podstawowych UE.

Konstytucja Rzeczypospolitej Polskiej. Pierwsze gwarancje ochrony danych osobowych zapewniła w Polsce Konstytucja z 1997 r. Jej art. 47 zagwarantował każdemu prawo do ochrony życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym (prawo do prywatności). Zgodnie zaś z art. 51, nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby, a władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym. Artykuł ten gwarantuje również każdemu prawo dostępu do dotyczących go urzędowych dokumentów i zbiorów danych (ograniczenie tego prawa może określić ustawa) oraz prawo do żądania sprostowania oraz usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą. Zasady i tryb gromadzenia oraz udostępniania informacji określać mogą wyłącznie przepisy rangi ustawy. Przepisem art. 51 Konstytucji zagwarantowana została autonomia informacyjna jednostki.

Ustawa o ochronie danych osobowych. Zasady ochrony danych ustanowione dyrektywą 95/46/WE wprowadzone zostały do polskiego porządku prawnego ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2015 r. poz. 2135, z późn. zm.). Ustawa ta zawiera szczegółowe normy służące ochronie danych osobowych w Polsce, a do dnia 1 maja 2004 r., czyli chwili wstąpienia Polski do Unii Europejskiej, przeniosła do polskiego porządku prawnego wszystkie zasady określone w dyrektywie 95/46/WE Parlamentu Europejskiego i Rady. Przepisy ustawy w pełni obowiązują od dnia 30 kwietnia 1998 roku.

Ustawa o ochronie danych osobowych określiła prawne ramy obrotu danymi osobowymi, a także zasady, jakie należy stosować przy ich przetwarzaniu, sprecyzowała też prawa i obowiązki tzw. administratorów danych, m.in. organów, instytucji i osób prowadzących zbiory danych osobowych oraz prawa osób, których dane dotyczą, w taki sposób, aby zagwarantować maksymalną ochronę praw i wolności każdej osobie fizycznej oraz poszanowania jej życia prywatnego.

Ustawa o ochronie danych osobowych, realizując wymagania stawiane przez prawo unijne, skonkretyzowała konstytucyjnie zagwarantowane prawo do decydowania o tym, komu, w jakim zakresie i w jakim celu przekazujemy nasze dane osobowe, dając ustawowe gwarancje przestrzegania tego prawa, poprzez wyposażenie osób, których dane dotyczą w środki służące realizacji tego prawa, a odpowiednie organy i służby w środki prawne, gwarantujące jego przestrzeganie. Podstawowym założeniem ustawy jest przyznanie każdej jednostce prawa do ochrony danych jej dotyczących.

2. REFORMA PRAWA UNII EUROPEJSKIEJ W ZAKRESIE OCHRONY DANYCH OSOBOWYCH

Odpowiedzią na liczne problemy związane z zapewnieniem właściwego poziomu ochrony danych osobowych oraz rozwój technologii związanych z ich przetwarzaniem, jak również coraz szersze pojmowanie pojęcia „dane osobowe" mają być nowe regulacje w tym zakresie. Obecnie na poziomie instytucji Unii Europejskiej zakończyły się negocjacje nowych unijnych zasad ochrony danych osobowych, przewidzianych ogólnym rozporządzeniem w sprawie ochrony danych osobowych oraz przepisami dyrektywy o ochronie danych w ramach działalności policyjnej i sądowej w sprawach karnych, co oznacza pilną konieczność podjęcia prac na poziomie krajowym w celu wdrożenia nowych przepisów.

Projekt rozporządzenia (zaprezentowany przez Komisję w styczniu 2012 r.) przewiduje szereg istotnych zmian, mających na celu wzmocnienie ochrony osób, których dane dotyczą. Obecne ramy ochrony danych osobowych są nadmiernie rozdrobnione i skomplikowane, z uwagi na fakt, iż dyrektywa 95/46/WE została implementowana w różny sposób w poszczególnych państwach członkowskich. Komisarz ds. Wymiaru Sprawiedliwości i Obywatelstwa Viviane Reding, prezentując projekt, wskazywała na konieczność zastąpienia tego „morza biurokracji" jednym prawem, które będzie obowiązywało w całej Unii Europejskiej.

Najważniejsze propozycje zmian, jakie znalazły się w projekcie z 2012 r. obejmowały następujące rozwiązania:

- Likwidacja wymogów administracyjnych, takich jak obowiązek zgłaszania zbiorów danych do rejestracji organom nadzorującym ochronę danych – zamiast tego projekt przewiduje większą odpowiedzialność i rozliczalność podmiotów przetwarzających dane osobowe (przykładowo przedsiębiorstwa i organizacje muszą powiadamiać krajowy organ nadzorczy o poważnych naruszeniach ochrony danych tak szybko, jak tylko jest to możliwe. Jeżeli jest to wykonalne, w ciągu 24 godzin).
- Administratorzy będą kontaktować się tylko z jednym krajowym organem nadzorującym ochronę danych, w tym państwie członkowskim UE, w którym posiadają główną siedzibę. Również osoby fizyczne będą mogły kontaktować się z organem ochrony danych w swoim państwie, nawet jeżeli ich dane są przetwarzane przez przedsiębiorstwo mające siedzibę poza UE. W przypadku gdy do przetwarzania danych konieczna jest zgoda, zostało zastrzeżone, że będzie ona musiała zostać wyrażona w sposób wyraźny, a nie być domniemana.
- „Prawo do bycia zapomnianym" pomoże podmiotom lepiej zarządzać ryzykiem związanym z ochroną danych w internecie: osoby fizyczne będą miały możliwość

usunięcia swoich danych, jeżeli nie będzie istnieć uzasadniona podstawa do ich zachowania.

- Unijne przepisy muszą obowiązywać w przypadku, gdy dane osobowe są przetwarzane zagranicą przez przedsiębiorstwa prowadzące działalność na rynku UE i oferujące swoje usługi obywatelom UE.
- Niezależne krajowe organy nadzorujące ochronę danych zostaną wzmocnione, aby mogły lepiej egzekwować unijne przepisy na terytorium kraju. Zostaną one upoważnione do nakładania kar na przedsiębiorstwa naruszające unijne przepisy o ochronie danych.
- Projekt Komisji obejmuje również wniosek ustawodawczy dotyczący dyrektywy w sprawie ochrony danych osobowych przetwarzanych na potrzeby zapobiegania przestępstwom, wykrywania ich, prowadzenia dochodzeń w ich sprawie i ich ścigania oraz powiązanych działań wymiaru sprawiedliwości w sprawach karnych. W nowej dyrektywie ogólne zasady ochrony danych zostaną zastosowane w odniesieniu do współpracy policyjnej i współpracy wymiarów sprawiedliwości w sprawach karnych. Przepisy dyrektywy będą miały zastosowanie do przekazywania danych zarówno w kraju, jak i do transferów transgranicznych.

Zanim jednak przepisy rozporządzenia zaczną funkcjonować w praktyce, podczas dwuletniego okresu przejściowego państwa członkowskie będą miały obowiązek dostosowania krajowych przepisów do nowych, zmodernizowanych i uaktualnionych zasad ochrony danych osobowych. Oznacza to nie tylko konieczność zmiany przepisów polskiej ustawy o ochronie danych osobowych (która nie będzie mogła powtarzać regulacji zawartych w unijnym rozporządzeniu), ale także zrewidowania i ewentualnego przekształcenia przepisów dotyczących danych osobowych, zawartych w innych aktach prawnych.

3. ROZWÓJ TECHNOLOGII I WYZWANIA ZWIĄZANE Z OCHRONĄ DANYCH OSOBOWYCH

Szybki rozwój nowych technologii przyniósł nowe wyzwania w zakresie ochrony danych osobowych. Skala pozyskiwania, gromadzenia i wymiany danych osobowych osiągnęła niebotyczne rozmiary. Z jednej strony jest to możliwe m.in. dzięki nowym, ciągle rozwijającym się technologiom, z których korzystają zarówno podmioty władzy publicznej, jak i przedsiębiorstwa prywatne. Z drugiej strony, osoby fizyczne coraz aktywniej udostępniają wiele informacji ze swojego życia prywatnego, a nawet intymnego, co powoduje, że stają się one publicznie dostępne. Fakt, że umieszczamy takie dane w internecie może prowadzić do wniosku, że mamy do niego zaufanie i nie zdajemy sobie sprawy z zagrożeń dla bezpieczeństwa danych osobowych, jakie ze sobą niesie zjawisko funkcjonowania tej globalnej sieci.

Korzystanie z nowoczesnych usług wręcz nierozerwalnie łączy się z udostępnianiem danych osobowych. Płatności przy użyciu kart kredytowych, zakupy przez internet, korzystanie z poczty elektronicznej, wyszukiwarek i portali społecznościowych czy używanie telefonów komórkowych - każda z tych zaledwie przykładowo wskazanych czynności wiąże się z udostępnianiem informacji na nasz temat. Informacje te mają różny stopień szczegółowości, różny charakter – od najdrobniejszych po najbardziej intymne - jednak przy obecnym poziomie rozwoju technologicznego do identyfikacji konkretnej osoby nie jest już niezbędne znanie jej imienia i nazwiska. Podkreślić przy tym należy, że w myśl art. 6 ust. 1 ustawy o ochronie danych osobowych, za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Przy zastosowaniu odpowiedniej techniki, możliwość zidentyfikowania osoby nawet za pomocą szczątkowych informacji staje się coraz łatwiejsza, zwłaszcza wobec coraz powszechniejszego łączenia danych pochodzących z różnych źródeł i wykorzystywania ich do nowych, w stosunku do pierwotnych, celów.

Wrażenie anonimowości w internecie obecnie pozostaje tylko iluzją. W rzeczywistości już samo wejście na stronę internetową wiąże się z wytwarzaniem i gromadzeniem danych, pozwalających na identyfikację bądź „wyodrębnienie" konkretnej osoby. Wszelkiego rodzaju aktywność w sieci – wyszukiwane hasła, odwiedzane strony, kupione produkty, poszczególne kliknięcia i wysyłane czy publikowane przez użytkownika informacje – są rejestrowane w postaci tzw. cyfrowych śladów oraz gromadzone na serwerach właścicieli stron i dostawców internetu. Źródłem informacji na temat konkretnych osób są również tzw. ciasteczka, czyli pliki cookies. Należy jednak poczynić rozróżnienie między plikami zapisywanymi na dysku użytkownika podczas korzystania ze stron internetowych, które pozwalają na zapamiętywanie np. haseł czy danych z wypełnianych formularzy, a plikami, których celem jest śledzenie aktywności internautów – tzw. *tracking cookies.*

Współcześnie dane osobowe stały się rodzajem „cyfrowej waluty", którą użytkownicy internetu muszą płacić za korzystanie z różnego rodzaju (w teorii darmowych) usług. Za pozyskiwanymi i analizowanymi w ten sposób informacjami stoi ogromna wartość ekonomiczna. Według badań wartość danych obywateli UE w 2011 r. wynosiła 315 mld euro. Do 2020 r. może ona wzrosnąć do blisko 1 bln euro rocznie. Jednocześnie w ogromnym tempie rośnie ilość dostępnych na rynku informacji o osobach dla porównania, dziś, w ciągu zaledwie dwóch dni, produkowane jest tyle danych, ile ludzkość wytworzyła do roku 2003.

Nic więc dziwnego, że obowiązujące w zakresie ochrony danych osobowych prawo przestało nadążać za rzeczywistością. Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych, która stanowi podstawę dla krajowych przepisów dotyczących ochrony danych osobowych, pochodzi z 1995 r. Tymczasem 20 lat temu dostęp do internetu posiadało zaledwie 0,8% światowej populacji, a dwa obecnie najpopularniejsze portale – Google i Facebook – miały powstać odpowiednio 3 i 9 lat później.

Wraz z ciągłym rozwojem technologii mnożą się nowe zagrożenia związane z ochroną danych osobowych przetwarzanych w coraz szerszym zakresie oraz na coraz nowsze sposoby. Jak wynika z przedstawionych w tym roku badań Eurobarometru, zaufanie obywateli do środowisk cyfrowych pozostaje na niskim poziomie. Dwie trzecie respondentów (67%) odpowiedziało, że martwi się faktem, iż nie mają kontroli nad informacjami, które podają w internecie, podczas gdy tylko 15% odpowiedziało, że mają nad nimi pełną kontrolę. Jednocześnie sześciu na dziesięciu respondentów wskazało, że nie ufa firmom internetowym (63%) czy też firmom telefonicznym oraz internetowym dostawcom usług (62%). Respondenci mają również poważne obawy co do konsekwencji gromadzenia, przetwarzania i wykorzystywania ich danych Siedem na dziesięć osób ma obawy co do wykorzystywania ich danych w celach innych niż ten, dla którego je pierwotnie zebrano.

3.1 PROFILOWANIE

Mechanizm profilowania Rada Europy w Rekomendacji CM/Rec (2010) 13 definiuje jako automatyczną technikę przetwarzania danych, polegającą na przypisaniu danej osobie „profilu", w celu podejmowania dotyczących jej decyzji bądź analizy lub przewidywania jej preferencji, zachowań i postaw. Profilowanie oznacza kategoryzowanie osób według różnych cech (np. płci, wieku, pochodzenia etnicznego, wzrostu) lub zachowań (np. nałogów, przyzwyczajeń, stylu życia, hobby) i wyciągnięcie na ich temat pewnych wniosków w oparciu o zebrane i przetworzone informacje.

Profilowanie, jako automatyczna operacja na danych, obarczone jest ryzykiem błędu – w efekcie, w odniesieniu do danej osoby mogą zostać przypisane założenia, które jej w rzeczywistości nie dotyczą. Do tego rodzaju operacji odnosi się art. 26a ust. 1 ustawy o ochronie danych osobowych, zgodnie z którym niedopuszczalne jest ostateczne rozstrzygnięcie indywidualnej sprawy osoby, której dane dotyczą, jeżeli jego treść jest wyłącznie wynikiem operacji na danych osobowych, prowadzonej w systemie informatycznym.

Profilowanie ma szerokie spektrum zastosowań. Przedsiębiorcy na podstawie otrzymanych profili mogą dopasować nie tylko reklamy, ale też same produkty i usługi do potrzeb konkretnych osób. Z mechanizmu profilowania chętnie korzystają również banki i ubezpieczyciele, zatem na jego podstawie mogą być podejmowane ważne dla obywateli decyzje, np. o przyznaniu ubezpieczenia lub kredytu. Przykładowo, wiek kierowcy może być jedną z cech, od której uzależniona jest wysokość składek OC za samochód, a nałóg nikotynowy – czynnikiem wpływającym na wysokość składki za ubezpieczenie zdrowotne.

Profilowanie jest także wykorzystywane przez sektor publiczny – policję i inne organy bezpieczeństwa oraz administrację w celu prowadzenia polityki społecznej. To właśnie ten mechanizm jest podstawą wyodrębniania spośród pasażerów linii lotniczych osób, które potencjalnie mogą stwarzać zagrożenie dla bezpieczeństwa publicznego. W polskim systemie prawnym przez pryzmat mechanizmu profilowania oceniana jest możliwość otrzymania przez bezrobotnego konkretnej formy pomocy. Takie rozwiązanie jest wynikiem reformy urzędów pracy, która weszła w życie w maju 2014 r. Generalny Inspektor zwracał uwagę, że proces ten, będący poważną ingerencją w sferę prywatności i autonomii informacyjnej jednostki, wymaga odpowiednich gwarancji w powszechnie obowiązującym prawie, których w żadnej mierze nie zapewniają obecnie obowiązujące przepisy.

Reforma unijnego prawa ochrony danych osobowych daje szansę na „ucywilizowanie" procesu profilowania. Wprowadzone mają zostać ograniczenia dotyczące profilowania, które wywołuje skutki prawne lub ma istotny wpływ na osobę fizyczną, a oparte jest wyłącznie na automatycznym przetwarzaniu danych. Profilowanie ma być dopuszczalne jedynie w ściśle określonych sytuacjach: podczas zawierania lub wykonania umowy, na podstawie przepisów prawa lub po uzyskaniu zgody podmiotu danych. Ponadto projekt przewiduje obowiązek poinformowania osoby, która podlega profilowaniu. Również art. 26a ust. 1 ustawy o ochronie danych osobowych zabrania dokonywania ostatecznych rozstrzygnięć indywidualnej sprawy osoby, której dane dotyczą, jeżeli jego treść jest wyłącznie wynikiem operacji na danych osobowych, prowadzonych w systemie informatycznym.

3.2 BIOMETRIA

Identyfikacja na podstawie danych biometrycznych bywa coraz częściej wykorzystywana np. w sektorze bankowym czy na potrzeby kontroli czasu pracy przez pracodawców. Metody biometryczne polegają na badaniu cech fizycznych (np. tęczówka oka, linie papilarne, kształt dłoni, układ żył w palcu czy nadgarstku, kształt małżowiny usznej, twarz, zapach), jak również cech związanych z zachowaniem (np. głos, sposób chodzenia, pisania na maszynie/klawiaturze, podpis odręczny). Dane biometryczne niewątpliwie można uznać za dane osobowe, jako pozwalające na ustalenie tożsamości określonej osoby w sposób pewny. Z racji ich wyłącznej przynależności do danej osoby, dane biometryczne stanowią pewnego rodzaju „identyfikator" człowieka. Dane te są niezmienne, co powoduje, że stanowią szczególny typ danych osobowych – dlatego do ich wykorzystywania należy podchodzić z dużą rozwagą, gdyż ich wyciek lub kradzież mogą mieć poważne w skutkach konsekwencje, nie tylko dla osób, których dane dotyczą.

Grupa Robocza art. 29[1] w dokumencie roboczym z 1 sierpnia 2003 r. dotyczącym biometrii wskazała, iż „(...) szybki rozwój technologii biometrycznych, jak i coraz powszechniejsze ich stosowanie w ostatnich latach, wymagają uważnej analizy z punktu widzenia ochrony danych. Powszechne i niekontrolowane posługiwanie się biometrią wzbudza niepokój z punktu widzenia ochrony wolności i fundamentalnych praw człowieka. (...) Szczególne zaniepokojenie związane z danymi biometrycznymi wzbudza ryzyko zmniejszenia wrażliwości ludzi, spowodowane coraz większą powszechnością używania tych danych, na konsekwencje, jakie przetwarzanie ich danych może mieć w ich życiu codziennym. (...) dane biometryczne zawsze mogą być uważane za «dane dotyczące osoby fizycznej», ponieważ odnoszą się do danych ze swej natury dotyczących określonej osoby".

Metoda identyfikacji biometrycznej w oparciu o próbkę głosu miała zostać wdrożona w nowym Systemie Informacji Telefonicznej, przygotowywanym przez Ministerstwo Finansów. Generalny Inspektor krytykował to rozwiązanie, wskazując, że korzystanie z tego systemu nie tylko jest nadmierną ingerencją w prywatność człowieka, ale też nie jest niezbędne w realizacji ustawowych zadań fiskusa, zarówno w przypadku przetwarzania informacji o podatnikach, jak i informacji o urzędnikach. Ponadto nie zostały stworzone stosowne przepisy, które mogłyby stanowić podstawę prawną dla funkcjonowania takiego systemu.

1 Grupa robocza ds. ochrony osób fizycznych w zakresie przetwarzania danych osobowych (Grupa Robocza art. 29) powołana została na mocy art. 29 dyrektywy 95/46/WE jako niezależny podmiot o charakterze doradczym. W skład Grupy Roboczej wchodzą przedstawiciele organu lub organów nadzorczych, powołanych przez każde Państwo Członkowskie, przedstawiciel organu lub organów ustanowionych dla instytucji i organów wspólnotowych oraz przedstawiciel Komisji.

3.3 „PRIVACY BY DEFAULT", „PRIVACY BY DESIGN", „PRIVACY IMPACT ASSESSMENT"

Koncepcja prywatności jako ustawienia domyślnego - *privacy by default* - oznacza, że ustawienia prywatności w urządzeniach, produktach lub usługach mają być nakierowane na maksymalną ochronę użytkownika i do niego ma należeć decyzja, czy i jakie dane chce udostępnić. Zgodnie z takim modelem, administrator danych ma obowiązek zapewnić, by domyślnie przetwarzane były tylko te dane, które są niezbędne dla realizacji zakładanego celu. Konieczne jest również zapewnienie, że w tzw. opcji domyślnej dane osobowe nie będą udostępniane nieograniczonej liczbie osób. Obecnie domyślne ustawienia kreowane są przez dostawców usług w sposób swobodny, zatem najczęściej zakładają one udostępnianie danych w możliwie najszerszym zakresie (przykładowo – domyślne ustawienia wszystkich informacji jako „publiczne" na portalu społecznościowym). Przekształcenie dotychczasowego modelu zagwarantowałoby przestrzeganie podstawowych zasad ochrony danych, przede wszystkim zasady adekwatności (zgodnie z którą dane powinny być adekwatne w stosunku do celów, w jakich są przetwarzane).

Każde przetwarzanie danych osobowych powinno być planowane z uwzględnieniem koncepcji ochrony prywatności w fazie projektowania (*privacy by design*). Idea *privacy by design* zrodziła się jako sposób spojrzenia na budowanie systemów teleinformatycznych. Polega ona na tym, by od samego początku tworzenia jakiegoś systemu, na każdym etapie, rozważać wpływ tworzonych rozwiązań na sferę prywatności i nie tyle odpowiadać na pojawiające się problemy, co wcześniej przewidywać najważniejsze z nich, analizując ryzyko wystąpienia określonych zdarzeń, czy dopuszczenia do zaniechań, i im przeciwdziałać.

Zasady *privacy by design* i *privacy by default* zostały zawarte również w przepisach procedowanego obecnie rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych. Ponadto, zgodnie z projektem rozporządzenia, jeśli operacje przetwarzania stwarzają szczególne ryzyko dla praw i wolności podmiotów danych z racji swego charakteru, zakresu lub celów, administrator lub podmiot przetwarzający przeprowadzają w imieniu administratora danych ocenę skutków przewidywanych operacji przetwarzania w zakresie ochrony danych osobowych (tzw. *privacy impact assessment*).

3.4 PRAWO DO BYCIA ZAPOMNIANYM (RIGHT TO BE FORGOTTEN)

Prawo do bycia zapomnianym (prawo żądania usunięcia danych) daje osobie, której dane dotyczą prawo – przy spełnieniu określonych warunków – do zaprzestania przetwarzania i usunięcia jego danych, zwłaszcza gdy brak jest uzasadnionego powodu do ich przechowywania. Rozwiązanie to nakłada na administratora danych obowiązek usunięcia danych określonej osoby, w przypadku otrzymania od niej odpowiedniego żądania, a następnie poinformowania osób trzecich również przetwarzających te dane o tym żądaniu oraz usunięcia wszelkich linków lub kopii tych danych osobowych.

Idea prawa do bycia zapomnianym związana jest z faktem, iż w internecie brak jest odpowiednika znanej z prawa karnego instytucji zatarcia skazania po upływie określonego czasu. „Wypowiedź, fotografia lub informacja o czynach staje się w internecie nieusuwalna, wpływając jednocześnie przez lata, bez ograniczenia czasowego, np. na karierę zawodową lub polityczną osoby, której dotyczy" (*M. Krzysztofek, „Prawo do bycia zapomnianym" i inne aspekty prywatności w epoce Internetu w prawie UE*, „Europejski Przegląd Sądowy", 2012/8). Dlatego też tak ważne jest wyposażenie obywateli w mechanizm realnej, skutecznej kontroli nad dotyczącymi ich informacjami udostępnionymi w internecie.

13 maja 2014 r., Trybunał Sprawiedliwości Unii Europejskiej wydał wyrok w sprawie Mario Costeja Gonzalez przeciwko Google Spain i Google Inc. (C-131/12). Orzeczenie to potwierdziło, iż operator wyszukiwarki internetowej w ramach swojej działalności nie tylko przetwarza dane osobowe, ale jest również ich administratorem, a zatem podmiotem, który decyduje o celach i środkach przetwarzania danych. Z tego powodu ciążą na nim określone obowiązki względem osób, których dane przetwarza – na wniosek podmiotu danych operator wyszukiwarki zobowiązany jest do usunięcia konkretnego linku z listy wyników wyszukiwania, jeżeli życzy sobie tego dany podmiot. Jeśli nie podejmie on odpowiednich działań, podmiot danych może zwrócić się do właściwego organu z wnioskiem o nakazanie usunięcia linku.

Prawo do bycia zapomnianym pozwala na bardziej efektywną kontrolę nad danymi przez osoby, których one dotyczą. Koncepcja ta stanowi jeden z filarów reformy europejskiego prawa ochrony danych osobowych, jak również spore wyzwanie, pojawiają się bowiem komentarze, że w praktyce realizacja tego prawa przez administratorów danych może okazać się zbyt skomplikowana.

3.5 PRZETWARZANIE DANYCH TELEKOMUNIKACYJNYCH PRZEZ POLICJĘ I SŁUŻBY

Problemy dotyczące okresu przechowywania (retencji) danych telekomunikacyjnych przez operatorów oraz granic inwigilacji obywateli przez służby od lat są przedmiotem zainteresowania Generalnego Inspektora. Zasadniczą kwestią w tym zakresie jest określenie, jak szeroki ma być dostęp służb do danych retencyjnych (tj. jakie rodzaje danych są pozyskiwane, techniczne aspekty ich zbierania, czas przechowywania) oraz w jaki sposób mógłby on być kontrolowany. W tym kontekście kluczowe znaczenie mają dwa wydane w 2014 r. wyroki – Trybunału Konstytucyjnego oraz Trybunału Sprawiedliwości Unii Europejskiej.

Trybunał Konstytucyjny w wyroku z dnia 30 lipca 2014 r. (sygn. akt K 23/11) za niezgodne z Konstytucją RP uznał przepisy ustaw o Policji i poszczególnych służbach, w zakresie, w jakim nie przewidują one niezależnej kontroli udostępniania danych telekomunikacyjnych. Zakwestionowane przepisy mają stracić moc obowiązującą po upływie 18 miesięcy od ogłoszenia wyroku, tj. w lutym 2016 r.

W lipcu 2015 r. Senat RP przedstawił projekt projektu ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw, który miał stanowić wykonanie wytycznych wynikających z wyżej wskazanego wyroku. Niestety, nie tylko w opinii GIODO, zaproponowana nowelizacja nie stwarzała wystarczających gwarancji ochrony prywatności i tajemnicy komunikowania się obywateli, a tym samym nie stanowiła pełnej realizacji wyroku Trybunału. W toku prac legislacyjnych organ wskazywał na szereg elementów, które powinny się znaleźć w nowych przepisach, tj. wprowadzenie jako zasady obowiązkowej, uprzedniej kontroli nad udostępnianiem danych telekomunikacyjnych; precyzyjne ograniczenie czasu przeprowadzania kontroli operacyjnej oraz przetwarzania danych telekomunikacyjnych; obowiązek poinformowania jednostki o podjętych wobec niej działaniach operacyjno rozpoznawczych oraz o pozyskaniu informacji na jej temat, a także możliwość pozyskiwania informacji o jednostkach tylko w przypadku poważnych przestępstw.

Ponadto kwestia sięgania przez Policję i służby po dane telekomunikacyjne nie może zostać uregulowana w sposób prawidłowy bez odniesienia się do wyroku Trybunału Sprawiedliwości Unii Europejskiej z dnia 8 kwietnia 2014 r., stwierdzającego nieważność całego aktu prawnego, jakim jest dyrektywa 2006/24 w sprawie zatrzymywania danych w połączonych sprawach C-293/12 i C-594/12 Digital Rights Ireland. Jako przyczynę nieważności dyrektywy 2006/24 w sprawie zatrzymywania danych Trybunał wskazał brak proporcjonalności zawartych w niej rozwiązań, które, mimo iż adekwatne do celu, jaki ma zostać za ich pomocą osiągnięty, ingerują zbyt głęboko w prawa podstawowe. TSUE uznał, że ten sam cel (zwalczanie poważnej przestępczości oraz zapewnienie

bezpieczeństwa publicznego) można było osiągnąć środkami, które w mniejszym stopniu ingerują w prawa jednostek. Mimo iż wyrok w sprawie Digital Rights Ireland nie powoduje automatycznie nieważności aktów prawa krajowego, implementujących dyrektywę 2006/24, to konieczne jest uwzględnienie go w pracach legislacyjnych nad przepisami ustawy, które dotyczą tej samej materii.

3.6 MONITORING WIZYJNY

Jedną z najbardziej problematycznych i wymagających uregulowania w przepisach prawa kwestii jest stosowanie monitoringu wizyjnego. W Polsce, podobnie jak w większości pozostałych państw europejskich, kamery monitoringu spotkać można na każdym kroku: na ulicach, w bankach, szkołach, szpitalach, obiektach sportowych czy sklepach. Z badań przeprowadzonych w 2012 r. przez Fundację Panoptykon we współpracy z Biurem Rzecznika Praw Obywatelskich wynika, że kamery miejskiego monitoringu wizyjnego zainstalowane są w 89 % polskich miast (miasta wojewódzkie i powiatowe), co już obrazuje skalę zjawiska.

Choć wideonadzór obecnie towarzyszy obywatelom niemal w każdej dziedzinie życia, wciąż nie został on kompleksowo unormowany na poziomie ustawy dedykowanej tej kwestii. Istnieją jedynie szczątkowe regulacje dotyczące niektórych aspektów działania monitoringu, np. w ustawie o Policji czy ustawie o strażach gminnych. Ustawa o ochronie danych osobowych nie reguluje w sposób szczególny kwestii przetwarzania danych wizualnych i dźwiękowych (choć niewątpliwie tego rodzaju informacje stanowić mogą dane osobowe). Monitorowanie zachowań osób, choć przez osoby stosujące takie rozwiązanie uzasadniane najczęściej względami bezpieczeństwa, silnie ingeruje w prywatność i jako takie powinno doczekać się kompleksowej regulacji, dotyczącej konkretnie tego zagadnienia – bowiem do kwestii związanych z monitoringiem wizyjnym, ze względu na ich specyfikę, nie zawsze jest możliwe dające wymierny efekt zastosowanie przepisów o ochronie danych osobowych. W 2011 r. Generalny Inspektor skierował w tej sprawie sygnalizację do Ministra Spraw Wewnętrznych i Administracji, wraz z opracowaniem „*Wymagania w zakresie regulacji monitoringu*". Generalny Inspektor wyraził wówczas stanowisko, iż konieczne jest zainicjowanie prac legislacyjnych, mających na celu unormowanie w przepisach rangi ustawowej ogólnych zasad i warunków dopuszczalności stosowania monitoringu wizyjnego, celów, do jakich może być wykorzystywany, a także okresu przechowywania nagrań i ich ewentualnego publikowania.

Wskazać w tym miejscu należy na opinię (nr 4/2004) Grupy Roboczej art. 29, w której zwrócono uwagę m.in. na konieczność respektowania zasady proporcjonalności (adekwatności) przy posługiwaniu się wideonadzorem, która oznacza przede wszystkim, że urządzenia monitoringu wizyjnego mogą być stosowane wyłącznie jako środki pomocnicze, gdy istnieje cel rzeczywiście uzasadniający ich użycie. Systemy te mogą być stosowane, gdy inne środki prewencyjne, ochrony lub bezpieczeństwa, nie wymagające pozyskiwania obrazu, okażą się ewidentnie niewystarczające lub niemożliwe do zastosowania w związku z powyższymi prawnie uzasadnionymi celami.

Istotne znaczenie ma w tej materii realizacja obowiązku informacyjnego wobec osób, których dane osobowe pozyskane zostały za pomocą monitoringu wizyjnego - osoby te muszą mieć świadomość faktu prowadzenia czynności wideonadzoru, tablice informacyjne o monitoringu wizyjnym powinny być widoczne i umieszczone w sposób trwały w niezbyt dużej odległości od nadzorowanych miejsc.

Warto w tym miejscu wspomnieć także o wyroku Trybunału Sprawiedliwości Unii Europejskiej w sprawie o sygn. C-212/13 Ryneš z dnia 11 grudnia 2014 r., w którym Trybunał uznał, iż wykorzystywanie systemu kamer monitoringu wizyjnego, zainstalowanego przez osobę fizyczną na jej domu rodzinnym, w celu ochrony własności, zdrowia i życia właścicieli domu, jako monitorującego również przestrzeń publiczną, nie stanowi wyłącznie przetwarzania danych w celach osobistych i domowych – a zatem nie zajdzie w tym przypadku wyłączenie stosowania przepisów o ochronie danych osobowych. Co istotne, TSUE nie kwestionował tego, że obraz osoby zarejestrowany przez kamerę, o ile pozwala ustalić jej tożsamość, stanowi dane osobowe w rozumieniu przepisów dyrektywy 95/46/WE.

3.7 PRZEKAZYWANIE DANYCH DO STANÓW ZJEDNOCZONYCH

Wielkie firmy internetowe, z Facebookiem i Google na czele, przetwarzają dane swoich użytkowników poza terenem Unii Europejskiej, co w praktyce negatywnie wpływa na interesy osób, których te dane dotyczą. Najbardziej jaskrawym przykładem są tu transfery danych do Stanów Zjednoczonych, bowiem już samo amerykańskie podejście do problematyki ochrony prywatności w znaczący sposób różni się od europejskiego. W przypadku USA mamy do czynienia z rozproszonymi przepisami o charakterze sektorowym – brak jest regulacji o charakterze ogólnym, która wiązałaby wszystkie podmioty, zarówno publiczne, jak i prywatne.

Z uwagi na różnice pomiędzy prawodawstwem Unii Europejskiej oraz Stanów Zjednoczonych, państwo to nie może zostać uznane za gwarantujące odpowiedni poziom ochrony danych osobowych. Mając na uwadze, że sytuacja taka w znacznym stopniu hamuje wymianę gospodarczą pomiędzy Unią Europejską a Stanami Zjednoczonymi Departament Handlu Stanów Zjednoczonych wypracował w 2000 r., w porozumieniu z Komisją Europejską, program *Safe Harbour* („bezpieczna przystań") umożliwiający amerykańskim podmiotom gospodarczym sprostanie wymaganiom unijnej dyrektywy. Uzyskanie certyfikatu programu *Safe Harbour* przez uczestniczące w nim podmioty miało zapewnić, że gwarantują one odpowiedni poziom ochrony danych osobowych, o którym mowa w dyrektywie 95/46/WE.

Praktyka pokazała jednak wiele niedoskonałości związanych z funkcjonowaniem programu. Jak wykazały przeprowadzone przez Komisję Europejską ewaluacje, nawet na podstawowym poziomie występowały problemy z przestrzeganiem jego zasad. Samo przekazanie danych do podmiotu legitymującego się certyfikatem *Safe Harbour* nie gwarantuje ponadto, że nie będą one wykorzystywane w inny sposób, np. przez organy ścigania.

W dniu 6 października 2015 r. Trybunał Sprawiedliwości Unii Europejskiej wydał przełomowy wyrok w sprawie Maximilian Schrems vs Data Protection Commissioner (C-362-14), w którym stwierdził nieważność decyzji Komisji Europejskiej w sprawie adekwatności zasad ochrony prywatności przewidzianych w ramach „bezpiecznej przystani" przez Stany Zjednoczone. To rozstrzygnięcie powoduje, że konieczne jest wypracowanie nowych, politycznych, prawnych i technicznych rozwiązań, umożliwiających przekazywanie danych na terytorium Stanów Zjednoczonych z poszanowaniem praw podstawowych. Skuteczne pozostają jednak wszystkie pozostałe przesłanki legalizujące transfer danych osobowych, nadal mogą być więc wykorzystywane standardowe klauzule umowne i Wiążące Reguły Korporacyjne, aczkolwiek problematyczna w indywidualnych przypadkach pozostaje kwestia, czy przesłanki te są w istocie stosowane w miejsce zasad wynikających z programu Safe Harbour, zakwestionowanych przez Trybunał.

3.8 KRADZIEŻ TOŻSAMOŚCI

Kradzież tożsamości często postrzegana jest jako sztuczny problem, z którym nigdy nie będziemy mieli do czynienia. Tymczasem każdy narażony jest na to, że ktoś skradnie jego tożsamość i, podszywając się pod inną osobę, zaciągnie w jej imieniu np. kredyt w banku. Źródła i sposoby pozyskiwania informacji o osobach mogą być i są bardzo różne, od kradzieży po wyłudzenie np. poprzez podszywanie się pod jakąś instytucję czy osobę. Przestępstwo kradzieży tożsamości ostatnio popełniane

jest na niespotykaną dotąd skalę. To właśnie jeden ze skutków żywiołowego rozwoju nowych technologii. Arkadiusz Lach, powołując się na źródła angielskie, wskazuje, że „(…) przywłaszczenie cudzej tożsamości jest określane przestępstwem Nowego Milenium, czyli przestępstwem Wieku Informacji" (*Karnoprawna reakcja na zjawisko kradzieży tożsamości*, Wolters Kluwer, Warszawa 2015).

W polskim prawie karnym niezbędną przesłanką dla uznania kradzieży tożsamości za działanie bezprawne jest wyrządzenie szkody osobistej lub materialnej poprzez wykorzystanie danych innej osoby. Stanowi o tym wprost art. 190a §2 Kodeksu karnego.

Zjawisko popełniania przestępstw związanych z kradzieżą tożsamości ma charakter niezwykle dynamiczny i stale rośnie, powodując wymierne straty. Według Raportu Komisji Europejskiej z 2015 r. zjawiskiem tym dotkniętych zostało około 2% mieszkańców UE, a średnia szkoda to 2500 euro. W Polsce, według badań przeprowadzonych przez TNS OBOP w 2008 r., jedynie 7% respondentów wskazało, iż padło ofiarą kradzieży tożsamości, podczas gdy w roku 2013 było to już 17%. Co istotne, aż 46% ofiar zadeklarowało, że konsekwencją bezprawnego wykorzystania ich danych osobowych była kradzież pieniędzy z ich rachunków bankowych.

Niezwykle istotnym elementem walki z tą przestępczością jest wzmożenie edukacji w zakresie prawa i zasad ochrony danych, w celu podnoszenia świadomości i wiedzy zarówno osób, których dane dotyczą, jak i podmiotów przetwarzających dane. Oprócz działalności edukacyjnej powinno się zainicjować stworzenie krajowej strategii ochrony przed tym coraz powszechniejszym zjawiskiem. W wielu państwach, m.in. w Australii, wprowadzono wydawanie certyfikatów dla pokrzywdzonych kradzieżą tożsamości po prawomocnym skazaniu sprawcy. Dzięki temu osoby, którym skradziono tożsamość, nie musiałyby składać wyjaśnień we wszystkich postępowaniach prowadzonych przez policję czy sąd (w miarę wykrywania kolejnych przestępstw dokonywanych przez osobę, która dokonała kradzieży danych). Wystarczyłoby bowiem jednorazowe oczyszczenie ich z zarzutu i odnotowanie tego np. w specjalnym rejestrze. Uchroniłoby to osoby poszkodowane przed czasochłonnymi i kosztownymi wizytami na policji czy w sądzie (często poza miejscem ich zamieszkania) a także usprawniło pracę wymiaru sprawiedliwości.

3.9 „INTERNET RZECZY”

„Internet Rzeczy”, inaczej „Internet Przedmiotów” (*Internet of Things*) to koncepcja, wedle której przedmioty mogą pośrednio albo bezpośrednio gromadzić, przetwarzać lub wymieniać dane za pośrednictwem sieci komputerowej. Do tego typu przedmiotów zaliczają się między innymi urządzenia grzewcze, gospodarstwa domowego, liczniki wody czy energii elektrycznej, ale również samochody, ubrania, a nawet artykuły spożywcze. Na rynku dostępne są także inteligentne urządzenia noszone na ciele lub w ciele człowieka – np. zliczające przebiegnięte kilometry, ale także mierzące poziom cukru czy monitorujące funkcjonowanie organizmu osoby chorej.

Z „Internetem Rzeczy” powiązana jest również idea „inteligentnego miasta” (*Smart City*), czyli miasta wykorzystującego rozwiązania teleinformatyczne dla lepszego funkcjonowania i zarządzania infrastrukturą miejską. Zastosowanie rozwiązań Smart City wiąże się również z gromadzeniem informacji, w tym danych osobowych, na temat mieszkańców i innych osób znajdujących się na terenie miasta.

Jak zwracała uwagę Grupa Robocza Art. 29 podczas prac nad opinią ws „Internetu Przedmiotów”, większość inteligentnych urządzeń nie jest projektowana z myślą o interoperacyjności, ale w celu przesyłania danych bezpośrednio do producenta urządzenia, który następnie staje się administratorem danych. Użytkownicy mogą uzyskać dostęp do swoich danych w sieci lub przy użyciu aplikacji w smartfonach, ale nie mogą zapobiec przekazywaniu danych do administratora danych. Podczas gdy istniejące urządzenia mierzą dane typowe dla środowiska, nowe urządzenia skupiają się bardziej na obserwacji zwyczajów użytkowników, zatem mogą obejmować przetwarzanie danych osobowych.

Choć wskazane wyżej koncepcje mogą przynieść różnego rodzaju ułatwienia w codziennym życiu – od drobnych udogodnień po ratowanie życia – wiążą się z nimi również potencjalne zagrożenia dla prywatności. Rozwój technologiczny nie powinien być hamowany, zwłaszcza jeśli w założeniu ma się on wiązać z pewnymi korzyściami dla jednostek i poprawą jakości życia, ale jednocześnie nie może odbywać się on kosztem ochrony danych osobowych. Konieczne jest zatem odpowiednie wyważenie wartości i zachowanie maksimum prywatności, nie umniejszając jednocześnie pozytywnych aspektów inteligentnych technologii.

Poniżej opisane zostaną – przykładowo – dwa wybrane zagadnienia związane z koncepcją „Internetu Rzeczy”, a mianowicie inteligentne liczniki energii elektrycznej oraz technologia RFID.

3.9.1 INTELIGENTNE LICZNIKI ENERGII – SMART GRID

Podstawowy model systemów energetycznych przechodzi w ostatnich latach głęboką przemianę. Dzięki technologii teleinformatycznej przeistoczył się ze względnie prostego układu dostawca – odbiorca, w układ zbliżony do rozproszonej sieci komputerowej o wielostronnym przepływie energii i informacji.

W założeniu zintegrowany system zbierania informacji o zużyciu prądu ma umożliwić bardziej świadome zarządzenie energią elektryczną. Z jednej strony dostawca będzie dokładnie wiedział, ile prądu potrzebujemy i dzięki temu będzie mógł ograniczać straty związane z przesyłem (istotne w globalnym wymiarze tego zjawiska). System zakłada także wprowadzenie zróżnicowanych taryf w zależności od tego, kiedy korzystamy z energii.

Z drugiej jednak strony, przy pomocy danych zebranych przez inteligentne liczniki i dokonanej na ich podstawie analizy schematów zachowań, można w łatwy sposób opracować profil osobowy użytkowników zamieszkałych pod danym adresem. W oparciu o wskazania licznika można ocenić, czy np. ktoś jest w domu, jakie ma zwyczaje, jakich urządzeń używa. Dlatego trzeba sobie zdawać sprawę, że zarówno na etapie tworzenia prawa dla tych systemów, jak i stosowania ich w praktyce, kwestie związane z ochroną prywatności powinny stanowić priorytet i być przedmiotem wnikliwej analizy, celem przyjęcia rozwiązań jak najmniej ingerujących w autonomię informacyjną i prywatność jednostek. Konieczne jest, przykładowo, ustalenie częstotliwości przesyłu danych, uzależnienie zakresu przekazywanych danych od celu, w jakim będą wykorzystywane oraz określenie czasu, przez który dane mają być przechowywane.

3.9.2 TECHNOLOGIA RFID

Technologia identyfikacji radiowej (ang. *Radio Frequency Identification* - RFID) umożliwia automatyczną identyfikację obiektów. Jej zastosowanie polega na wykorzystaniu miniaturowych urządzeń zwanych znacznikami lub tagami RFID. Wyposaża się w nie coraz więcej przedmiotów, m.in. towary w sklepach. Dzięki zainstalowaniu takich mikroprocesorów, które mogą być odczytywane bezprzewodowo za pomocą fal radiowych, możliwe jest pozyskiwanie wiedzy zarówno na temat wyposażonych w nie przedmiotów, jak i osób, które je użytkują. Najczęściej odbywa się to nie tylko bez naszej zgody, ale i wiedzy, co rodzi zagrożenia dla naszej prywatności.

Systemy RFID są obecnie powszechnie wykorzystywane m.in. do zabezpieczania towarów przed kradzieżami. Ponadto technologia ta pozwala na gromadzenie rozmaitych danych dotyczących określonej osoby, śledzenie obywateli poruszających się w miejscach publicznych, takich jak np. lotniska, centra handlowe, dworce, ulice. Jej zastosowanie daje możliwość wzbogacania profili poprzez monitorowanie zachowań konsumentów w sklepach, odczytywania informacji m.in. o noszonych ubraniach i używanych akcesoriach.

Zwolennicy tych rozwiązań podnoszą liczne ich zalety, jak np. kwestie bezpieczeństwa. Obawy jednak wzbudza możliwość zdalnej identyfikacji lub uzyskania dostępu do informacji przez osoby do tego nieupoważnione.

Według przyjętych przez Komisję Europejską zaleceń, państwa członkowskie powinny zagwarantować skuteczne mechanizmy ochrony danych osobowych przetwarzanych przy wykorzystaniu technologii RFID. W szczególności przedstawiciele sektora handlu detalicznego zobowiązani zostali do informowania osób fizycznych - poprzez stosowanie wspólnego znaku europejskiego – o identyfikatorach umieszczonych lub wbudowanych w produkty. Przy sprzedaży identyfikatory te powinny być dezaktywowane lub usuwane, chyba że konsumenci wyrażą zgodę na dalsze ich działanie.

Konieczna jest również lepsza edukacja osób, których stosowanie technologii RFID może dotyczyć.

3.10 CENTRALNE ZBIORY DANYCH OSOBOWYCH

W związku z dynamicznym rozwojem technologii i informatyzacją administracji publicznej, coraz częściej tworzone są różnego rodzaju państwowe rejestry, dzięki którym liczne podmioty w szerokim zakresie mogą przetwarzać informacje o obywatelach.

Tego typu centralne systemy stworzone zostały w sektorze szkolnictwa (System Informacji Oświatowej) oraz w sektorze ochrony zdrowia (System Informacji Medycznej). W państwowych rejestrach przetwarzane są również m.in. dane osób bezrobotnych czy korzystających z pomocy społecznej. Wskazać można ponadto na prowadzoną przez Ministerstwo Sprawiedliwości elektroniczną Centralną Bazę Danych Ksiąg Wieczystych.

Konstruowanie wielkich publicznych baz danych nie może odbywać się bez uwzględnienia wpływu tworzonego systemu na prywatność osób fizycznych i z pominięciem zasad wynikających z przepisów Konstytucji RP, ustawy o ochronie danych osobowych i wydanych na jej podstawie rozporządzeń wykonawczych. Każdorazowo takie działania muszą mieć miejsce z uwzględnieniem koncepcji opisanych w punkcie 2.3. Istotne jest, by to w przepisach rangi ustawy regulowane były zasadnicze kwestie związane z funkcjonowaniem rejestru, a mianowicie katalog przetwarzanych danych, okres ich przechowywania, zasady udostępniania informacji z rejestru, czy też krąg podmiotów mających dostęp do danych. Zasada prymatu przepisów ustawowych wynika również ze stanowisk Trybunału Konstytucyjnego, m.in. w postanowieniu z dnia 31 stycznia 2007 r. (sygnatura S 1/2007) Trybunał wskazał, iż „zasadnicza regulacja pewnej kwestii nie może być domeną przepisów wykonawczych, wydawanych przez organy nie należące do władzy ustawodawczej. Nie jest bowiem dopuszczalne, aby prawodawczym decyzjom organu władzy wykonawczej pozostawić kształtowanie zasadniczych elementów regulacji prawnej". Wymóg umieszczenia bezpośrednio w ustawie wszystkich zasadniczych elementów regulacji prawnej musi być stosowany ze szczególnym rygoryzmem, gdy regulacja ta dotyczy korzystania przez obywateli z ich praw i wolności (wyrok Trybunału Konstytucyjnego z dnia 25 maja 1998 r., sygnatura U 19/97). Podobnie orzekł Trybunał w wyroku z dnia 18 grudnia 2014 r. (sygnatura K 33/13), dotyczącym tworzenia rejestrów danych medycznych na podstawie rozporządzenia Ministra Zdrowia.

Dopiero sformułowanie właściwych zasad w przepisach ustawy (dedykowanej danemu zagadnieniu czy sektorowi albo działowi administracji) stwarza podstawy do funkcjonowania danego rejestru. W praktyce często jednak okazuje się, że w pierwszej kolejności dokonywany jest zakup systemu informatycznego, do którego następnie dopasowywane są tworzone regulacje prawne. Niejednokrotnie u podstaw tworzenia rejestrów znajdują się akty niższego rzędu niż ustawa bądź też regulacje pozaustawowe (porozumienia, umowy, wytyczne, itp.), co jest niezgodne z konstytucyjną zasadą legalizmu (art. 51 Konstytucji RP).

Pojawiają się także wątpliwości związane z dopuszczalnością przekazywania danych osobowych między różnymi rejestrami. Bywa, że do dokonywania takich operacji- w miejsce tworzenia właściwych przepisów prawa w tym zakresie - wykorzystywana jest instytucja powierzenia przetwarzania danych osobowych (uregulowana w art. 31 ustawy o ochronie danych osobowych), co jest niezgodne z obowiązującym prawem. Należy bowiem podkreślić, że powierzenie przetwarzania danych osobowych oznacza dokonywanie na danych operacji jedynie w imieniu i na rzecz ich administratora, i nie może prowadzić do zmiany jego statusu, tj. podejmowania przez podmiot, któremu powierzono przetwarzanie danych, jakichkolwiek operacji na tych danych, które to działania prowadziłyby do realizacji własnych celów lub interesów tegoż podmiotu. Administrator nie może powierzyć innemu podmiotowi przetwarzania danych w celu innym niż ten, dla którego on je przetwarza.

Doprowadziłoby to bowiem do sytuacji, w której administrator przeniósłby na inny podmiot uprawnienia, których sam nie posiada. Nie może także dochodzić mocą umowy cywilno-prawnej do cedowania uprawnień poszczególnych organów czy regulowania mocą umowy kwestii podstawowych, jakimi są zasady przetwarzania danych osobowych, które regulować mogą jedynie przepisy powszechnie obowiązującego prawa, zwłaszcza w przypadku przetwarzania danych szczególnie chronionych. Stosowaną na poziomie centralnym, niedopuszczalną z punktu widzenia ochrony danych osobowych, praktyką jest kopiowanie istniejących zbiorów, by mógł z nich skorzystać inny podmiot, zamiast czerpania z dostępnych rozwiązań – obowiązujących przepisów prawa określających zasady dostępu do informacji zawartych w danym zbiorze.

Z tychże względów tworzenie rejestrów zawierających dane osobowe musi być poprzedzone dokładną analizą wpływu projektowanych rozwiązań na ochronę danych, co jest szczególnie ważne zwłaszcza w przypadku centralnych zbiorów danych, administrowanych przez podmioty publiczne, które mają obowiązek działać na podstawie i w granicach przepisów powszechnie obowiązującego prawa, kompleksowo regulujących istnienie tychże zbiorów i zasady przetwarzania informacji o osobach (m.in. wskazujących warunki zasilania centralnych baz, czerpania z ich zasobów, czy też retencji danych w nich zawartych).

Podkreślić należy, iż GIODO będzie zwracał szczególną uwagę na kwestie związane z funkcjonowaniem istniejących, a także dopiero projektowanych rejestrów o charakterze centralnym. Związana z tym będzie analiza zasadności gromadzenia danych na poziomie centralnym, bowiem nie w każdym przypadku konieczny jest taki dostęp do szerokiego katalogu informacji o osobie. Tam, gdzie to możliwe, powinien być zaproponowany inny model realizacji określonych zadań, tak aby przetwarzanie określonych danych osobowych na poziomie centralnym miało miejsce wyłącznie wtedy, gdy jest rzeczywiście niezbędne z uwagi na wskazany w przepisach prawa cel.

3.11 PONOWNE WYKORZYSTANIE INFORMACJI PUBLICZNEJ

Udostępnienie informacji znajdujących się w zasobach administracji publicznej do powtórnego wykorzystania rodzi pewne obawy związane z ochroną naszych danych. Dotyczą one przede wszystkim tego, że może dochodzić do nieuprawnionego łączenia danych osobowych, które pochodzą z różnych zbiorów będących w posiadaniu administracji publicznej.

Zgodnie z przepisami prawa Unii Europejskiej co do zasady obecnie obowiązkowe jest, aby organy sektora publicznego pozwalały na ponowne wykorzystywanie wszystkich informacji, które posiadają, zarówno do celów komercyjnych, jak i niekomercyjnych

(wynika to z dyrektywy 2003/98/WE Parlamentu Europejskiego i Rady z dnia 17 listopada 2003 r. w sprawie ponownego wykorzystywania informacji sektora publicznego, nazywanej również „dyrektywą reuse").

Jak wskazała Grupa Robocza Art. 29 w opinii 06/2013, ponowne wykorzystywanie informacji sektora publicznego może przynieść korzyści społeczeństwu, w tym większą przejrzystość sektora publicznego oraz przyczynienie się do innowacyjności. Niemniej jednak zwiększenie dostępności informacji publicznych, szczególnie gdy obejmują one dane osobowe, nie pozostaje bez wiążących się z tym zagrożeń. Dlatego też istotne jest posiadanie solidnej podstawy prawnej do publicznego udostępniania danych osobowych, z uwzględnieniem istotnych zasad ochrony danych, w tym zasad proporcjonalności, ograniczenia celu oraz minimalizacji zakresu danych. W celu zapewnienia odpowiednich zabezpieczeń zaleca się przeprowadzenie oceny wpływu na ochronę danych, zanim informacje sektora publicznego obejmujące dane osobowe zostaną udostępnione do ponownego wykorzystania.

Przepisy dotyczące ponownego wykorzystania informacji publicznej w praktyce umożliwiają podmiotom spoza sektora administracji publicznej łączenie danych pochodzących z jawnych rejestrów, które do tej pory były prowadzone wyłącznie przez władzę publiczną. Pewien niepokój budzi w tym kontekście brak rozróżnienia w polskim prawie pomiędzy jawnością formalną danych, które mogą stanowić informację publiczną, a tak zwaną „otwartością", która nie jest w polskim prawie zdefiniowana. Brak definicji otwartości prowadzić może do traktowania informacji jawnej formalnie jako informacji możliwej do dowolnego przetwarzania.

Jako przykład posłużyć mogą tu dane z elektronicznych ksiąg wieczystych oraz dane z Krajowego Rejestru Sądowego, zawierające np. informacje o numerze PESEL poszczególnych osób fizycznych. Jeżeli połączymy je z danymi z innych rejestrów, np. z powszechnie dostępnego rejestru pośredników w handlu nieruchomościami, zawierającego dane o imieniu, nazwisku i miejscu zamieszkania pośrednika, to otrzymamy wyraźny profil konkretnej osoby. Informacja przekazana do ponownego wykorzystania może służyć do profilowania osoby fizycznej i wyciągania z kształtu takiego profilu wniosków, które mogą prowadzić np. do dyskryminacji osoby.

Przy łączeniu w nowych zbiorach danych pochodzących z publicznych rejestrów nadal konieczne jest przestrzeganie zasad ochrony danych osobowych, czego nie zawsze są świadomi przetwarzający takie dane, przede wszystkim wypełnienie obowiązku informacyjnego wobec osób, których dane dotyczą. Brak informacji co do źródeł pozyskania danych o osobie i o celach, w jakich są udostępniane uniemożliwia skorzystanie z prawa żądania usunięcia danych czy też złożenia sprzeciwu wobec ich przetwarzania.

3.12 „BIG DATA”

Big Data (Duże zbiory danych) to gigantyczne zbiory danych cyfrowych będące w posiadaniu przedsiębiorstw, rządów i innych dużych organizacji, które są poddawane szczegółowej analizie przy użyciu algorytmów komputerowych. Często uznaje się, że możliwość przechowywania i analizowania ogromnych ilości danych może okazać się przydatna dla społeczeństwa. Big Data mogą być wykorzystywane na przykład do przewidywania rozpowszechniania się epidemii, wykrywania poważnych skutków ubocznych lekarstw oraz zwalczania zanieczyszczenia środowiska w dużych miastach. Niektóre z tych zastosowań nie wiążą się z danymi osobowymi; jednakże Big Data mogą być również wykorzystywane w sposoby budzące istotne obawy co do ochrony prywatności osób i praw obywatelskich, ochrony przed dyskryminacyjnymi skutkami oraz naruszeniami prawa do równego traktowania.

Analityka biznesowa danych nie jest sama w sobie zakazana. Trzeba jednak pamiętać, że gdy dotyczy danych objętych ochroną, zarówno przez prawo ochrony danych osobowych, jak i w związku z istnieniem tajemnic prawnie chronionych – jak np. tajemnica bankowa lub telekomunikacyjna – posiadacze takich danych nie mogą się nimi swobodnie dzielić. Nie można także ich łączyć. Prawo zabrania zestawiania danych pozyskanych na różne potrzeby bez zgody osób, których one dotyczą lub bez innej wyraźnej podstawy prawnej. Zgoda ta musi być świadoma, niewymuszona, poprzedzona obowiązkiem informacyjnym. Tymczasem obserwowane jest przez podmioty biznesowe umiejętne ukrywanie informacji mających na celu podanie rzeczywistego celu ich pozyskiwania od osób zainteresowanych.

Niepokojącą kwestią jest również analityka predykcyjna, w której z cech uważanych za prawdziwe albo uprawdopodobnione, próbujemy wnioskować o cechach, które jeszcze uprawdopodobnione nie są. Takie działanie jest dopuszczalne wyłącznie w sytuacji, gdy wymaga tego prawo albo w sytuacji, gdy istnieje zgoda ze strony osoby zainteresowanej. Musi być ona jednak poinformowana, że takie działania są podejmowane, na czym polegają oraz zawsze powinna mieć dostęp do informacji o tym, jakie dane na jej temat są zbierane i w jaki sposób są przetwarzane.

***

Powyższe kwestie należy uznać za jedne z tych, które w ocenie Generalnego Inspektora Ochrony Danych Osobowych uważane są za znaczące, jeśli chodzi o wyzwania związane z zapewnieniem ochrony danych osobowych. Ze względu na ich znaczenie – zarówno w odniesieniu do sposobu funkcjonowania instytucji publicznych, jak i podmiotów komercyjnych – winny być one przedmiotem zainteresowania organu stojącego na straży zasad ochrony danych osobowych.

4. ZADANIA GENERALNEGO INSPEKTORA OCHRONY DANYCH OSOBOWYCH I POTRZEBA ZMIAN

W obliczu mających nastąpić zmian i związanych z tym licznych wyzwań, uzasadnione wydaje się przypomnienie miejsca i roli Generalnego Inspektora Ochrony Danych Osobowych w polskim porządku prawnym. Podkreślić należy, że ustanowienie organu wynika wprost z przepisów prawa Unii Europejskiej (dyrektywy 95/46/WE), które to wyznaczają również w sposób ramowy jego zadania i kompetencje. W świetle przepisów ustawy o ochronie danych osobowych, stanowiących implementację unijnej dyrektywy do polskiego porządku prawnego, GIODO jest uprawniony do:

- kontroli zgodności przetwarzania danych z przepisami o ochronie danych osobowych,
- wydawania decyzji administracyjnych i rozpatrywania skarg w sprawach wykonania przepisów o ochronie danych osobowych,
- zapewnienia wykonania przez zobowiązanych obowiązków o charakterze niepieniężnym wynikających z decyzji, o których mowa w pkt 2, przez stosowanie środków egzekucyjnych przewidzianych w ustawie z dnia 17 czerwca 1966 r. o postępowaniu egzekucyjnym w administracji (Dz. U. z 2005 r. Nr 229, poz. 1954, z późn. zm.),
- prowadzenia rejestru zbiorów danych oraz rejestru administratorów bezpieczeństwa informacji, a także udzielania informacji o zarejestrowanych zbiorach danych i zarejestrowanych administratorach bezpieczeństwa informacji,
- opiniowania projektów ustaw i rozporządzeń dotyczących ochrony danych osobowych,
- inicjowania i podejmowania przedsięwzięć w zakresie doskonalenia ochrony danych osobowych,
- uczestniczenia w pracach międzynarodowych organizacji i instytucji zajmujących się problematyką ochrony danych osobowych (art. 12 ustawy).

Nie są to jednak jedyne zadania należące do organu. Dodatkowe obowiązki GIODO wynikają również m.in. z dyrektywy 2002/58/WE o prywatności i łączności elektronicznej, dyrektywy 2000/31/WE dotyczącej handlu elektronicznego, Decyzji ramowej 2008/977/WSiSW w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych czy też Decyzji Rady nr 2009/371/WSiSW z dnia 6 kwietnia 2009 r. ustanawiającej Europejski Urząd Policji (Europol). W lipcu 2016 r. wejdzie w życie Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (tzw. rozporządzenie eIDAS), które również będzie się wiązało z nowymi zadaniami dla GIODO.

Wskazane wyżej europejskie regulacje mają konkretne przełożenie na przepisy polskich aktów prawnych i funkcjonowanie Biura GIODO. Na mocy przepisów ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz. U. z 2014 r. poz. 243, z późn. zm.) dostawcy publicznie dostępnych usług telekomunikacyjnych, w przypadku stwierdzenia naruszenia bezpieczeństwa danych osobowych, zobowiązani są w szczególności powiadomić o tym właściwy organ ds. ochrony danych osobowych. W związku z powyższym wyznaczeni przez Generalnego Inspektora pracownicy Biura GIODO wykonują zadanie organizacji i koordynacji przyjmowania oraz rozpatrywania zawiadomień o naruszeniu danych osobowych w oparciu o opracowaną instrukcję postępowania.

Ważny aspekt działalności organu wynika ponadto z przepisów ustawy z dnia 24 sierpnia 2007 r. o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym (Dz. U. z 2014 r. poz. 1203, z późn. zm.). Zgodnie z art. 8 ust. 1 tej ustawy Generalny Inspektor sprawuje kontrolę nad tym, czy wykorzystywanie danych (przetwarzanych w wyżej wskazanych systemach) nie narusza praw osób, których dane te dotyczą. W 2014 r. GIODO przeprowadził 20 kontroli dotyczących przetwarzania danych osobowych w Krajowym Systemie Informatycznym (KSI), umożliwiającym organom administracji publicznej i organom wymiaru sprawiedliwości wykorzystywanie danych gromadzonych w Systemie Informacyjnym Schengen oraz w Wizowym Systemie Informacyjnym. Tego typu kontrole zostały przeprowadzone w Komendzie Głównej Policji, Biurze Ochrony Rządu, jednostkach Żandarmerii Wojskowej, sądach, prokuraturach oraz w konsulatach przy ambasadach Rzeczypospolitej Polskiej.

GIODO prowadzi również działania edukacyjne, jest m.in. autorem ogólnopolskiego programu edukacyjnego „Twoje dane - Twoja sprawa. Skuteczna ochrona danych osobowych. Inicjatywa edukacyjna skierowana do uczniów i nauczycieli", który ma na celu uwrażliwienie nauczycieli i uczniów na zagrożenia, jakie dla ochrony danych osobowych i prywatności istnieją w codziennym korzystaniu z internetu. Statystycznie rocznie przystępuje do niego ponad 200 placówek, a w jego realizację włączonych jest ok. 4000 nauczycieli oraz 30000 uczniów w całej Polsce. W roku szkolnym 2015/2016 realizowana jest szósta edycja tego projektu, w której uczestniczy 250 placówek. Jednocześnie Generalny Inspektor Ochrony Danych Osobowych współpracuje w ramach podpisanych porozumień o współpracy w zakresie ochrony prywatności i danych osobowych z 17 uczelniami wyższymi w Polsce.

Ponadto w ramach współpracy GIODO z innymi instytucjami i organizacjami, podpisane zostały porozumienia o wspólnym działaniu na rzecz podnoszenia standardów ochrony danych osobowych i prawa do prywatności, a także wypracowane zostały kodeksy dobrych praktyk w dziedzinie ochrony danych osobowych.

Powyższe wiąże się również z uczestnictwem Generalnego Inspektora i przedstawicieli organu w różnego rodzaju spotkaniach, konferencjach i debatach, co ma na celu upowszechnianie wiedzy na temat zasad ochrony danych osobowych.

Urząd podejmuje ponadto szereg działań w ramach współpracy międzynarodowej, do których należy udział w posiedzeniach Grupy Roboczej Art. 29 ds. ochrony danych osobowych, w tym w pracach podgrup tematycznych, udział w pracach Komitetu Konsultacyjnego Rady Europy, współpraca z rzecznikami ochrony danych innych krajów – w szczególności w ramach Grupy Rzeczników Ochrony Danych Osobowych Państw Europy Środkowej i Wschodniej, której jest założycielem, i w której pełni rolę Sekretariatu, oraz udział w organizowanych cyklicznie Międzynarodowych Konferencjach Rzeczników Ochrony Danych i Prywatności, Wiosennych Konferencjach Europejskich Organów Ochrony Danych oraz w Warsztatach Rozpatrywania Spraw. Inne ważne zadania stojące przed polskim organem ds. ochrony danych w ramach współpracy międzynarodowej, związane są z jego udziałem w pracach grup koordynujących nadzór nad SIS II, VIS, CIS oraz IMI, grupy koordynacyjnej do spraw nadzoru nad systemem Eurodac, Systemem Informacji Celnej, wspólnego organu nadzorczego Europolu, a także Grupy roboczej ds. ochrony danych osobowych w Telekomunikacji (tzw. Grupa Berlińska).

Aktywność GIODO na przestrzeni blisko 18 lat funkcjonowania urzędu w zauważalny sposób wpłynęła na podniesienie poziomu świadomości społeczeństwa w kwestiach związanych z ochroną danych osobowych. Jest to widoczne zarówno jeśli chodzi o obecność tych zagadnień w debacie publicznej, jak i coraz liczniej kierowane do organu skargi dotyczące naruszenia przepisów o ochronie danych osobowych oraz zapytania z prośbą o interpretację obowiązujących w obszarze ochrony danych osobowych przepisów prawa, bądź sygnalizujących różnego rodzaju problemy interpretacyjne związane z ich przestrzeganiem.

***

W ostatnich latach znacząco wzrosło obciążenie urzędu, szczególnie biorąc pod uwagę liczbę otrzymywanych przede wszystkim od osób, których dane dotyczą, skarg na nieprawidłowości w związku z przetwarzaniem danych osobowych. W 2014 r. do Generalnego Inspektora skierowano ponad 4,5 tysiąca pytań z prośbą o interpretację przepisów prawa i blisko 2,5 tysiąca skarg. Dla porównania – w 2007 r. było to odpowiednio ok. 1,7 tysiąca pytań i prawie 800 skarg[2]. Innym ważnym zadaniem, a jednocześnie wyzwaniem dla GIODO jest rejestracja zbiorów danych osobowych. W 2014 r. do rejestracji zgłoszono ponad 43 tysiące zbiorów, podczas gdy w 2007 r. było to zaledwie niecałe 5 tysięcy. Od 2015 r. urząd zajmuje się również

2 Szczegółowe statystyki dotyczące działalności Biura GIODO w latach 2007 – 2014 zawierają załączniki do pisma.

rejestracją administratorów bezpieczeństwa informacji – zgodnie z nowelizacją ustawy o ochronie danych osobowych, jeżeli administrator danych skorzysta z przysługującego mu uprawnienia i powoła administratora bezpieczeństwa informacji, ma 30 dni od dnia powołania ABI na zgłoszenie tego faktu do rejestracji Generalnemu Inspektorowi.

Tymczasem zatrudnienie w latach 2007 – 2014 wzrosło jedynie o 12 osób (ze 120 zatrudnionych na dzień 31 grudnia 2007 r. do 132 na dzień 31 stycznia 2014 r.). Budżet Generalnego Inspektora ustalony w ustawie budżetowej na 2007 r. wynosił: 12 391 tys. zł (w tym 8 152 tys. zł przeznaczone na wynagrodzenia), a w ustawie budżetowej na 2014 r. – 15 225 tys. zł (9 351 tys. zł na wynagrodzenia).

Obserwując wzrastającą liczbę spraw, którymi organ obowiązany jest się zajmować, uzasadniony wydaje się być wniosek, że bez pewnych zmian systemowych coraz trudniej będzie sprostać wszystkim wyzwaniom. Szansą na podniesienie poziomu realnego przestrzegania przepisów jest wzmocnienie pozycji organu ochrony danych osobowych i przyznanie mu kompetencji do nakładania kar finansowych, co wynika z planowanej reformy unijnych regulacji. Obecnie GIODO nie posiada uprawnień do nakładania kar finansowych, co w praktyce niejednokrotnie wpływa negatywnie na skuteczność działań. Sytuację dodatkowo komplikuje fakt, iż urząd nie posiada oddziałów terenowych i dysponuje jedynie 14 inspektorami (przeprowadzającymi działania kontrolne zgodnie z art. 12 pkt 1 ustawy o ochronie danych osobowych) w skali kraju. Dla porównania, PIP posiada 1700 inspektorów oraz kilka tysięcy społecznych inspektorów pracy. Z kolei system ochrony praw konsumentów opiera się na miejskich i powiatowych rzecznikach konsumentów.

W związku z powyższym, zdaniem organu, w praktyce musi zostać wzmocniona również pozycja obecnych administratorów bezpieczeństwa informacji (ABI). Zgodnie z nowym unijnym rozporządzeniem będą to urzędnicy ochrony danych osobowych (data protection officers – DPO). Generalny Inspektor widzi realną potrzebę współpracy z tymi podmiotami. Do tej pory do Biura GIODO wpłynęło blisko 23 000 zgłoszeń powołania ABI, zarejestrowano zaś niemal 16 000 ABI (liczba ta powinna sukcesywnie rosnąć).

W związku z ostatnią nowelizacją ustawy o ochronie danych osobowych wprowadzone zostały zmiany m.in. w zakresie funkcjonowania administratora bezpieczeństwa informacji. Instytucja ABI nie jest nową konstrukcją w polskim porządku prawnym. Pozycja ABI wyznaczona została przepisami obowiązującej aktualnie dyrektywy 95/46/WE. Przyjęte w nowelizacji rozwiązania mają również na celu przygotowanie administratorów danych do unormowań zapowiadanych w projekcie rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony

osób fizycznych, w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. W obecnym stanie prawnym powołanie administratora bezpieczeństwa informacji jest fakultatywne, jednak po wejściu w życie unijnego rozporządzenia i wprowadzeniu funkcji urzędnika ochrony danych – DPO, zastępującej ABI, stanie się to obowiązkowe. Niepowołanie administratora bezpieczeństwa informacji skutkuje tym, że w razie zaistnienia nieprawidłowości związanych z przetwarzaniem danych osobowych, to administrator danych osobowych (czyli np. minister w przypadku rejestrów o charakterze centralnym) ponosi pełną odpowiedzialność z tego tytułu - również karną, na podstawie przepisów Rozdziału 8 ustawy o ochronie danych osobowych.

Zgodnie z obowiązującymi od początku 2015 r. przepisami znowelizowanej ustawy o ochronie danych osobowych, jednym z zadań ABI jest obecnie sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania dla administratora danych. W ocenie organu, działalność ABI w tym zakresie, może pomóc w zapewnieniu wyższego poziomu ochrony danych osobowych. Pod tym względem Generalny Inspektor widzi w administratorach bezpieczeństwa informacji swoich partnerów, a nawet podmioty, które w pierwszej kolejności mogłyby reagować na nieprawidłowości dotyczące przetwarzania danych u administratorów danych osobowych, którzy ich powołali. Konieczne jest jednak do tego odpowiednie przygotowanie merytoryczne oraz wola współpracy z organem ochrony danych osobowych. Administratorzy bezpieczeństwa informacji mogą być pewnego rodzaju łącznikami na bieżąco współpracującymi z GIODO, przy jednoczesnym zachowaniu ich pełnej niezależności.

Wzmocnienie poziomu ochrony w ramach struktur administratorów danych osobowych i administratorów bezpieczeństwa informacji jest potrzebne również ze względu na fakt, iż Generalny Inspektor bywa traktowany jak podmiot do świadczenia obsługi prawnej administratorów danych osobowych, zarówno z sektora publicznego, jak i prywatnego. Biuro często otrzymuje pytania dotyczące rozwiązań organizacyjnych, jakie powinien przyjąć administrator danych, czy podejmowanych przez niego decyzji. Tymczasem takie rozstrzygnięcia nie leżą w kompetencji GIODO, bowiem to administrator danych osobowych, jako podmiot decydujący o celach i środkach przetwarzania danych osobowych, powinien zapewniać przestrzeganie przepisów o ochronie danych osobowych oraz stosować odpowiednie do swojej struktury, realizowanych zadań, zakresu przetwarzanych danych osobowych (zarówno kategorie danych, jak i skala ich przetwarzania) środki techniczne i organizacyjne w tym zakresie, w tym w postaci administratora bezpieczeństwa informacji. GIODO ma kompetencje do kontroli przyjętych rozwiązań, a nie zastępowania podmiotów, które powinny przestrzegać zasad ochrony danych osobowych w realizacji ich obowiązków.

Doświadczenie Generalnego Inspektora pokazuje również, że pomimo istnienia w przepisie art. 12 pkt 5 stosownej kompetencji, nie wszystkie projekty aktów normatywnych istotnych z punktu widzenia ochrony danych osobowych są przedstawiane organowi do zaopiniowania (dotyczy to zarówno projektów rozporządzeń, ustaw, jak i umów międzynarodowych). Bywa, że GIODO jest włączany w proces legislacyjny dopiero na etapie prac parlamentarnych, zdarza się również, że jest całkowicie pomijany podczas konsultacji treści projektów, które bezpośrednio wiążą się z kwestią ochrony danych osobowych. Konieczne jest zatem monitorowanie na bieżąco przez pracowników biura wszystkich projektów aktów normatywnych, które mogą mieć związek z tym zagadnieniem, co często jest zadaniem wysoce utrudnionym z uwagi na ich ilość.

Rola organu w procesie legislacyjnym bywa ponadto niewłaściwie rozumiana - w odpowiedzi na zgłaszane zastrzeżenia z punktu widzenia zgodności z ustawą o ochronie danych osobowych, projektodawcy często oczekują od GIODO sformułowania gotowych propozycji brzmienia przepisów. Tymczasem organ do spraw ochrony danych osobowych może jedynie wskazać kierunki potencjalnych rozwiązań i pełnić funkcję doradczą, natomiast sformułowanie konkretnych rozwiązań legislacyjnych należy do projektodawcy – tym bardziej, że to projektodawca powinien dysponować wiedzą dotyczącą celów przetwarzania danych oraz na temat tego, do jakiego rodzaju danych potrzebny jest dostęp, biorąc pod uwagę realizację zadań wynikających z projektowanych przepisów. Pierwsza ocena w tym zakresie powinna należeć do administratorów bezpieczeństwa informacji funkcjonujących w ramach poszczególnych resortów.

Tego rodzaju analiza powinna zostać przeprowadzona z uwzględnieniem wynikających z nowego rozporządzenia ogólnego Unii Europejskiej koncepcji *privacy by default* oraz *privacy by design* i dokonaniem oceny skutków projektowanych rozwiązań na prywatność jednostek (*privacy impact assessment*).

Generalny Inspektor może zatem wyrazić opinię co do zgodności projektowanych przepisów z przepisami ustawy ochrony danych osobowych i pełnić w procesie formułowania przepisów funkcję partnera projektodawcy, a nie kolejnego twórcy przepisów. GIODO, jako organ niezależny, nieznajdujący się w strukturze rządowej, nie posiada również inicjatywy ustawodawczej, co ewentualnie uzasadniałoby oczekiwania dotyczące przedstawiania przez niego poprawek legislacyjnych.

Ograniczone możliwości działania GIODO wynikają jednak nie tylko z wyżej wspomnianego braku inicjatywy ustawodawczej. Generalnemu Inspektorowi nie przysługuje także prawo do złożenia do Trybunału Konstytucyjnego wniosku o stwierdzenie niezgodności przepisów prawa, wydawanych przez centralne organy

państwowe, z Konstytucją RP, ratyfikowanymi umowami międzynarodowymi i ustawami. W znaczący sposób ogranicza to możliwość działania, w przypadku gdy zostały uchwalone przepisy, co do których na etapie prac rządowych lub parlamentarnych organ zgłaszał uwagi dotyczące ich niezgodności z Konstytucją i ustawą o ochronie danych osobowych. Organ nie posiada ponadto uprawnień do skierowania do Naczelnego Sądu Administracyjnego wniosku o podjęcie uchwały w celu wyjaśnienia przepisów prawa materialnego lub procesowego, których stosowanie wywołało rozbieżności w orzecznictwie sądów administracyjnych. Na pozycję organu negatywnie oddziałuje także brak jego umocowania w przepisach Konstytucji RP – tak jak ma to miejsce w przypadku Rzecznika Praw Obywatelskich czy Rzecznika Praw Dziecka.

Ponadto również z uwagi na przyszłe regulacje prawa Unii Europejskiej, konieczne będzie opracowanie nowej koncepcji statusu prawno-organizacyjnego Generalnego Inspektora Ochrony Danych Osobowych.

***

Przetwarzanie danych osobowych z zachowaniem odpowiednich środków ostrożności i z poszanowaniem zasad wynikających z obowiązujących przepisów prawa jest konieczne nie tylko ze względu na ochronę prywatności jednostek, ale także z uwagi na zapewnienie bezpieczeństwa państwa, rozumianego jako bezpieczeństwo przepływu informacji.

Niniejsze opracowanie ma na celu pokazanie jak szeroki jest zakres obowiązków spoczywających na Generalnym Inspektorze Ochrony Danych Osobowych i jak różnorodne są zagadnienia, z którymi urząd spotyka się w praktyce. Przez blisko 18 lat obowiązywania ustawy o ochronie danych osobowych w polskim porządku prawnym obszar działalności organu znacząco ewoluował, przy niezmiennych, a zatem ograniczonych możliwościach działania organu i nieadekwatnej liczbowo obsadzie kadrowej. By zatem zwiększyć efektywność działania urzędu, co jest potrzebne zwłaszcza z uwagi na opisane wyżej wyzwania związane z rozwojem technologii i przyszłe, ale nieodległe, rozwiązania prawne na poziomie rozporządzenia ogólnego, konieczne jest nowe spojrzenie na rolę Generalnego Inspektora i przekształcenie jej tak, by odpowiadała zarówno wymogom wynikającym z przepisów prawa Unii Europejskiej, jak i potrzebom osób, których dane dotyczą. Niewątpliwie jest to ogromne wyzwanie, które stoi zarówno przed podmiotami opracowującymi projekty aktów prawnych, ustawodawcą, jak również adresatami tychże przepisów. Jego realizacja nie będzie jednak możliwa bez wprowadzenia stosownych zmian w przepisach prawa oraz bez dysponowania odpowiednimi środkami do urzeczywistnienia tychże zadań. Jednocześnie organ deklaruje chęć współpracy i aktywnego udziału w pracach mających na celu doprowadzenie do powstania konkretnych rozwiązań prawnych.

GIODO

Generalny Inspektor
Ochrony Danych Osobowych

Biuro Generalnego Inspektora Ochrony Danych Osobowych
ul. Stawki 2, 00-193 Warszawa
tel. 22 531 03 00
fax. 22 531 03 01
kancelaria@giodo.gov.pl